DETAILED ACTION

1. Applicant's response filed on July 28, 2011 has been fully considered. Independent claims 1, 8, 15, and 21 have been amended. Claim 7 has been canceled. Claims 1, 3-4, 8, 10-11, 15, 17, 21, 23-24, 28-30, and 33-36 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3-4, 8, 10-11, 21, 23-24, 28-30, and 33-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arrow et al. (U.S. Patent No. 6,175,917 B1), hereinafter "Arrow", in view of Sullenberger et al. (U.S. Patent No. 7,447,901 B1), hereinafter "Sullengerger", and further in view of Bisbee et al. (U.S. Patent No. 7,657,531 B2), hereinafter "Bisbee".

Referring to claim 1:

i. Arrow teaches:

A network comprising:

IP processing apparatuses, which use an IP (Internet Protocol) for encrypting and authenticating communications via the Internet between two different centers (see figure 1, elements 115, 125, 135, 145, 155; and column 6, line 61, through column 7, line 7, of Arrow); and

an IP setting apparatus, which manages IP settings of the IP processing apparatuses (see figure 1, element 160 'VPN management station'; figure 13, elements 1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15, of Arrow);

wherein in response to receiving a request from a first IP processing apparatus to communicate with a second IP processing apparatus, the second IP processing apparatus transmits a response (see column 7, lines 26-45, of Arrow);

wherein said IP setting apparatus generates SA (Security Association) parameters, to be used in the IP communication between the first and the second IP processing apparatuses, based on the contents of the request message and contents of IP policies stored by the IP setting apparatus (see figure 13, 1310 'define VPN parameters [i.e., generating Security Association (SA) parameters]', 1314 'define access control rules [i.e., generating IP policies]', of Arrow);

wherein said IP setting apparatus sends a distribution message including the policies of said IP and the SA parameters in response to the request message (see column 12, lines 22-25 'manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160', of Arrow).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

Arrow discloses that the VPN management unit issues a request to a VPN unit for configuration (see column 12, lines 22-25 'configuration module 710 of operating system 116 manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160.', of Arrow, emphasis added). Arrow further discloses that the VPN unit sends a request message to the VPN management unit (see column 12, line 25 'it also reports configuration status information concerning host VPN unit 115 to VPN management station 160', of Arrow). However, Arrow does not specifically mention that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit.

Arrow discloses that the IP setting apparatus generates and transmits encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses (see col. 6, lines 31-34, 'VPN management station [i.e., IP setting apparatus] 160 controls VPN units [i.e., IP process apparatuses] 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100.'; col. 9, lines 35-40 'Configuration data includes information used to operate VPN unit 115, such as: an IP address of the unit, IP addresses of VPN endstations that will be transmitting data through the unit, the encryption algorithm [i.e., including the generated encryption key] to be used, the authentication algorithm to be used,'; and col. 11, lines 27-30 'RSA module 722 supports management of encryption keys [i.e., included in the configuration data] and loading of configuration information into VPN unit 115 from VPN management station 160 (from FIG. 1).', of Arrow). However, Arrow does not explicitly disclose the common encryption key.

Arrow does not explicitly disclose IPsec processing apparatus retransmits the request for communication to the IPsec setting apparatus and receives new setting information before a term of validity for the SA expires.

ii. Sullenberger teaches a method for establishing a dynamic multipoint encryption virtual private network, wherein Sullenberger that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit to dynamically establish an encrypted virtual private network (see figure 1; column 7, line 63 to column 8, line 3; and column 10, lines 38-51, of Sullenberger).

Sullenberger further discloses the IPsec protocol (see column 1, lines 50-59, of Sullenberger), the common encryption key (see column 2, lines 24-29 'establishing a shared secret [i.e., generating and transmitting the common encryption key] between the two endpoints'; and column 7, lines 44-47 'the encryption methodology is DES [i.e., DES (Data Encryption Standard) using the common encryption key]', of Sullenberger), and the specific key lifetime values (see coumn 7, line 46, of Sullengerger).

On the hand, Bisbee teaches a method for state-less authentication, wherein Bisbee discloses IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires (see column 11, lines 1-7 'The Security Context and the symmetric session encryption key contained therein are then forwarded to the User and retained for the period for which the Security Context is valid. In some instances, the Time-Offset and Expiration Time values may also be returned to the User, which allows the User to **renew** the Security Context prior to its **expiration** [i.e., IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires].', of Bisbee).

In addition, Bisbee further discloses a setting apparatus generating and transmitting common encryption keys to the process apparatuses to be used to encrypt and authenticate IP communications (see col. 10, line 66 to col. 11, line 4 'The Security Context Body is then encrypted using the Logon Component-specified symmetric or the generated private key [i.e., generating common encryption key] referenced by the respective Key Handle. The Security Context and the symmetric session encryption key [i.e., the common encryption key] contained therein are then forwarded to the User [i.e., transmitting the generated common encryption key, e.g. to the first and second IP process apparatuses] and retained for the period for which the Security Context is valid.', of Bisbee).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Sullenberger into the system of Arrow such that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit and dynamically establish an encrypted virtual private network, because Arrow teaches "VPN management station 160 controls VPN units 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100." (see column 6, lines 31-34, of Arrow, emphasis added). Sullenberger teaches "The invention relates more specifically to a method and apparatus for establishing a **dynamic** multipoint encrypted virtual private network

(VPN)." (see column 1, lines 19-21, of Sullenberger, emphasis added). Therefore, Sullenberger's teaching could enhance Arrow's system.

The ordinary skilled person would have been motivated to have applied the teaching of Bisbee into the system of Arrow such that a VPN unit retransmitts a request to the VPN management unit before a term of validity for the SA expires, because Arrow teaches defining Security Associations (SA) for a VPN unit (see figure 13, 1310 'define VPN parameters', of Arrow). Therefore, Bisbee's teaching could increase the network security for Arrow's system, because Bisbee requires a VPN unit retransmitts a request to the VPN management unit before a term of validity for the SA expires.

Referring to claims 3-4, 10-11, 23-24, 29:

Arrow, Sullenberger, and Bisbee teach the claimed subject matter: a network (see claim 1 above). They further disclose transmitting messages between IPsec setting server apparatus and IPsec processing apparatus (see column 9, lines 19-22 of Arrow).

Referring to claim 8:

i. Arrow teaches:

An IP setting apparatus managing IP setting of IP processing apparatuses, which use an IP (Internet Protocol) for securing communication via the Internet between two different centers (see figure 1, element 160; figure 13, elements 1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15, of Arrow),

wherein said IP setting apparatus manages IP policies applied among IP processing apparatus(see figure 1, element 160; figure 13, elements 1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15 of Arrow);

wherein said IP setting apparatus includes means for specifying the IP policies of said IP to be applied between a first IP processing apparatus and the second IP processing apparatus (see figure 11, element 1102 'receive request to configure VPN unit'; figure 13, elements 1310 'define VPN parameters [i.e., Security

Association (SA)', 1314 'define access control rules', 1316 'define address translation rules'; and column 15, line 52-column 16, line 15, of Arrow, emphasis added).

wherein said IP setting apparatus generates SA (Security Association) parameters, to be used in the IP communication between the first and the second IP processing apparatuses, based on the contents of the request message and contents of IP policies stored by the IP setting apparatus (see figure 13, 1310 'define VPN parameters [i.e., generating Security Association (SA) parameters]', 1314 'define access control rules [i.e., generating IP policies]', of Arrow); and

wherein said IP setting apparatus sends a distribution message including the policies of said IP and the SA parameters in response to the request message (see column 12, lines 22-25 'manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160', of Arrow).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

Arrow discloses that the VPN management unit issues a request to a VPN unit for configuration (see column 12, lines 22-25 'configuration module 710 of operating system 116 manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160.', of Arrow, emphasis added). Arrow further discloses that the VPN unit sends a request message to the VPN management unit (see column 12, line 25 'it also reports configuration status information concerning host VPN unit 115 to VPN management station 160', of Arrow). However, Arrow does not specifically mention that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit.

Arrow discloses that the IP setting apparatus generates and transmits encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses (see col. 6, lines 31-34, 'VPN management station [i.e., IP setting apparatus] 160 controls VPN units [i.e., IP process apparatuses] 115, 125 and 135

through commands and configuration information transmitted to the respective VPN unit through public network 100.'; col. 9, lines 35-40 'Configuration data includes information used to operate VPN unit 115, such as: an IP address of the unit, IP addresses of VPN endstations that will be transmitting data through the unit, the encryption algorithm [i.e., including the generated encryption key] to be used, the authentication algorithm to be used,'; and col. 11, lines 27-30 'RSA module 722 supports management of encryption keys [i.e., included in the configuration data] and loading of configuration information into VPN unit 115 from VPN management station 160 (from FIG. 1).', of Arrow). However, Arrow does not explicitly disclose the common encryption key.

Arrow does not explicitly disclose IPsec processing apparatus retransmits the request for communication to the IPsec setting apparatus and receives new setting information before a term of validity for the SA expires.

ii. Sullenberger teaches a method for establishing a dynamic multipoint encryption virtual private network, wherein Sullenberger that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit to dynamically establish an encrypted virtual private network (see figure 1; column 7, line 63 to column 8, line 3; and column 10, lines 38-51, of Sullenberger).

Sullenberger further discloses the IPsec protocol (see column 1, lines 50-59, of Sullenberger), the common encryption key (see column 2, lines 24-29 'establishing a shared secret [i.e., generating and transmitting the common encryption key] between the two endpoints'; and column 7, lines 44-47 'the encryption methodology is DES [i.e., DES (Data Encryption Standard) using the common encryption key]', of Sullenberger), and the specific key lifetime values (see coumn 7, line 46, of Sullengerger).

On the hand, Bisbee teaches a method for state-less authentication, wherein Bisbee discloses IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires (see column 11, lines 1-7 'The Security Context and the symmetric session encryption key contained therein are then forwarded to the User and retained for the period for which the Security Context is valid.

In some instances, the Time-Offset and Expiration Time values may also be returned to the User, which allows the User to **renew** the Security Context prior to its **expiration** [i.e., IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires].', of Bisbee).

In addition, Bisbee further discloses a setting apparatus generating and transmitting common encryption keys to the process apparatuses to be used to encrypt and authenticate IP communications (see col. 10, line 66 to col. 11, line 4 'The Security Context Body is then encrypted using the Logon Component-specified symmetric or the generated private key [i.e., generating common encryption key] referenced by the respective Key Handle. The Security Context and the symmetric session encryption key [i.e., the common encryption key] contained therein are then forwarded to the User [i.e., transmitting the generated common encryption key, e.g. to the first and second IP process apparatuses] and retained for the period for which the Security Context is valid.', of Bisbee).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Sullenberger into the system of Arrow such that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit and dynamically establish an encrypted virtual private network, because Arrow teaches "VPN management station 160 controls VPN units 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100." (see column 6, lines 31-34, of Arrow, emphasis added). Sullenberger teaches "The invention relates more specifically to a method and apparatus for establishing a **dynamic** multipoint encrypted virtual private network (VPN)." (see column 1, lines 19-21, of Sullenberger, emphasis added). Therefore, Sullenberger's teaching could enhance Arrow's system.

The ordinary skilled person would have been motivated to have applied the teaching of Bisbee into the system of Arrow such that a VPN unit retransmitts a request to the VPN management unit before a term of validity for the SA expires, because Arrow teaches defining Security Associations (SA) for a VPN unit (see

figure 13, 1310 'define VPN parameters', of Arrow). Therefore, Bisbee's teaching could increase the network security for Arrow's system, because Bisbee requires a VPN unit retransmitts a request to the VPN management unit before a term of validity for the SA expires.

Referring to claim 30:

Arrow, Sullenberger, and Bisbee teach the claimed subject matter: an IPsec processing apparatus (see claim 15 above). They further disclose the SPD [i.e., Security Policy Database], SAD [i.e., Security Association Database] (see figure 2, elements 203 'IPSec Policy', 124C 'security association', of Sullenberger).

Referring to claim 21:

i. Arrow teaches:

An IPsec setting method comprising:

receiving from IP processing apparatus a request (see column 14, lines 33-44, of Arrow),

retrieving IP policy rules from memory and generating IP settings parameters based on the content of the request from the IP processing apparatus and the retrieved policy rules (see column 14, lines 33-44, of Arrow); and

transmitting the generated IP settings to the IP processing apparatus (see column 14, lines 33-44, of Arrow),

wherein said IP setting apparatus generates SA (Security Association) parameters, to be used in the IP communication between the first and the second IP processing apparatuses, based on the contents of the request message and contents of IP policies stored by the IP setting apparatus (see figure 13, 1310 'define VPN parameters [i.e., generating Security Association (SA) parameters]', 1314 'define access control rules [i.e., generating IP policies]', of Arrow);

wherein said IP setting apparatus sends a distribution message including the policies of said IP and the SA parameters in response to the request message (see column 12, lines 22-25 'manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160', of Arrow).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

Arrow discloses that the VPN management unit issues a request to a VPN unit for configuration (see column 12, lines 22-25 'configuration module 710 of operating system 116 manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160.', of Arrow, emphasis added). Arrow further discloses that the VPN unit sends a request message to the VPN management unit (see column 12, line 25 'it also reports configuration status information concerning host VPN unit 115 to VPN management station 160', of Arrow). However, Arrow does not specifically mention that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit.

Arrow discloses that the IP setting apparatus generates and transmits encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses (see col. 6, lines 31-34, 'VPN management station [i.e., IP setting apparatus] 160 controls VPN units [i.e., IP process apparatuses] 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100.'; col. 9, lines 35-40 'Configuration data includes information used to operate VPN unit 115, such as: an IP address of the unit, IP addresses of VPN endstations that will be transmitting data through the unit, the encryption algorithm [i.e., including the generated encryption key] to be used, the authentication algorithm to be used,'; and col. 11, lines 27-30 'RSA module 722 supports management of encryption keys [i.e., included in the configuration data] and loading of configuration information into VPN unit 115 from VPN management station 160 (from FIG. 1).', of Arrow). However, Arrow does not explicitly disclose the common encryption key.

Arrow does not explicitly disclose IPsec processing apparatus retransmits the request for communication to the IPsec setting apparatus and receives new setting information before a term of validity for the SA expires.

ii. Sullenberger teaches a method for establishing a dynamic multipoint encryption virtual private network, wherein Sullenberger that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit to dynamically establish an encrypted virtual private network (see figure 1; column 7, line 63 to column 8, line 3; and column 10, lines 38-51, of Sullenberger).

Sullenberger further discloses the IPsec protocol (see column 1, lines 50-59, of Sullenberger), the common encryption key (see column 2, lines 24-29 'establishing a shared secret [i.e., generating and transmitting the common encryption key] between the two endpoints'; and column 7, lines 44-47 'the encryption methodology is DES [i.e., DES (Data Encryption Standard) using the common encryption key]', of Sullenberger), and the specific key lifetime values (see coumn 7, line 46, of Sullengerger).

On the hand, Bisbee teaches a method for state-less authentication, wherein Bisbee discloses IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires (see column 11, lines 1-7 'The Security Context and the symmetric session encryption key contained therein are then forwarded to the User and retained for the period for which the Security Context is valid. In some instances, the Time-Offset and Expiration Time values may also be returned to the User, which allows the User to **renew** the Security Context prior to its **expiration** [i.e., IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires].', of Bisbee).

In addition, Bisbee further discloses a setting apparatus generating and transmitting common encryption keys to the process apparatuses to be used to encrypt and authenticate IP communications (see col. 10, line 66 to col. 11, line 4 'The Security Context Body is then encrypted using the Logon Component-specified symmetric or the generated private key [i.e., generating common encryption key] referenced by the respective Key Handle. The Security Context and the symmetric session encryption key [i.e., the common encryption key] contained therein are then

forwarded to the User [i.e., transmitting the generated common encryption key, e.g. to the first and second IP process apparatuses] and retained for the period for which the Security Context is valid.', of Bisbee).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Sullenberger into the system of Arrow such that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit and dynamically establish an encrypted virtual private network, because Arrow teaches "VPN management station 160 controls VPN units 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100." (see column 6, lines 31-34, of Arrow, emphasis added). Sullenberger teaches "The invention relates more specifically to a method and apparatus for establishing a **dynamic** multipoint encrypted virtual private network (VPN)." (see column 1, lines 19-21, of Sullenberger, emphasis added). Therefore, Sullenberger's teaching could enhance Arrow's system.

The ordinary skilled person would have been motivated to have applied the teaching of Bisbee into the system of Arrow such that a VPN unit retransmitts a request to the VPN management unit before a term of validity for the SA expires, because Arrow teaches defining Security Associations (SA) for a VPN unit (see figure 13, 1310 'define VPN parameters', of Arrow). Therefore, Bisbee's teaching could increase the network security for Arrow's system, because Bisbee requires a VPN unit retransmitts a request to the VPN management unit before a term of validity for the SA expires.

Referring to claim 28:

Arrow, Sullenberger, and Bisbee teach the claimed subject matter: an IPsec setting method (see claim 21 above). They further disclose the inquiry means (see column 14, line 25, of Arrow).

Referring to claims 33-35:

Arrow, Sullenberger, and Bisbee teach the claimed subject matter: a network (see claim 1 above). They further discloses transmitting the encryption key to the first and the second IPsec processing apparatus depending on their addresses (see

column 9, lines 18-22, of Arrow), and the common encrypt key (see column 2, lines 24-29; and column 7, lines 44-47, of Sullenberger).

Referring to claim 36:

Arrow, Sullenberger, and Bisbee teach the claimed subject matter: a network (see claim 1 above). They further discloses the encrypted communication (see column 11, lines 43-45, of Arrow).

4. Claims 15, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arrow et al. (U.S. Patent No. 6,175,917 B1), in view of Sullenberger et al. (U.S. Patent No. 7,447,901 B1), further in view of Bisbee et al. (U.S. Patent No. 7,657,531 B2), and further in view of Park et al. (U.S. Pub. No. 2003/0126466 A1).

Referring to claim 15:

i. Arrow teaches:

An IP processing apparatus using an IP (Internet Protocol) on the Internet,

wherein said IP processing apparatus receives from an IP setting apparatus managing communication a packet containing the IP to be applied to communication with another IP processing apparatus, determines whether or not to request from the IP setting apparatus a setting for IP communication (see column 4, lines 38-40; column 11, lines 27-30 of Arrow), and

wherein the IP processing apparatus transmits a request to the IP setting apparatus in order to receive from the IP setting apparatus a setting for IP communication (see figure 11, element 1102 'receive request to configure VPN unit'; figure 13, elements 1310 'define VPN parameters', 1314 'define access control rules', 1316 'define address translation rules'; and column 15, line 52-column 16, line 15, of Arrow, emphasis added),

wherein said IP processing apparatus includes means for setting an SPD (Security Processing Database), in which policies for applying said IP is recorded, and an SAD (Security Association Database), in which an SA (security

Association) necessary for subjecting an individual communication to the IP processing is stored, based upon a message received from the IP setting apparatus (see column 13, lines 60-64 'database 906 [i.e., SPD/SAD]; and figure 13, 1310 'define VPN parameters [i.e., generating Security Association (SA) parameters]', 1314 'define access control rules [i.e., generating IP policies]', of Arrow);

wherein said IP setting apparatus sends a distribution message including the policies of said IP and the SA parameters in response to the request message (see column 12, lines 22-25 'manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160', of Arrow).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

Arrow discloses that the VPN management unit issues a request to a VPN unit for configuration (see column 12, lines 22-25 'configuration module 710 of operating system 116 manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160.', of Arrow, emphasis added). Arrow further discloses that the VPN unit sends a request message to the VPN management unit (see column 12, line 25 'it also reports configuration status information concerning host VPN unit 115 to VPN management station 160', of Arrow). However, Arrow does not specifically mention that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit.

Arrow discloses that the IP setting apparatus generates and transmits encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses (see col. 6, lines 31-34, 'VPN management station [i.e., IP setting apparatus] 160 controls VPN units [i.e., IP process apparatuses] 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100.'; col. 9, lines 35-40 'Configuration data includes information used to operate VPN unit 115, such as: an IP address of the unit, IP addresses of VPN

endstations that will be transmitting data through the unit, the encryption algorithm [i.e., including the generated encryption key] to be used, the authentication algorithm to be used,'; and col. 11, lines 27-30 'RSA module 722 supports management of encryption keys [i.e., included in the configuration data] and loading of configuration information into VPN unit 115 from VPN management station 160 (from FIG. 1).', of Arrow). However, Arrow does not explicitly disclose the common encryption key.

Arrow does not explicitly disclose IPsec processing apparatus retransmits the request for communication to the IPsec setting apparatus and receives new setting information before a term of validity for the SA expires.

Arrow discloses the database. However, Arrow does not explicitly disclose the SPD (Security Processing Database) and SAD (Security Association Database).

ii. Sullenberger teaches a method for establishing a dynamic multipoint encryption virtual private network, wherein Sullenberger that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit to dynamically establish an encrypted virtual private network (see figure 1; column 7, line 63 to column 8, line 3; and column 10, lines 38-51, of Sullenberger).

Sullenberger further discloses the IPsec protocol (see column 1, lines 50-59, of Sullenberger), the common encryption key (see column 2, lines 24-29 'establishing a shared secret [i.e., generating and transmitting the common encryption key] between the two endpoints'; and column 7, lines 44-47 'the encryption methodology is DES [i.e., DES (Data Encryption Standard) using the common encryption key]', of Sullenberger), and the specific key lifetime values (see coumn 7, line 46, of Sullengerger).

On the hand, Bisbee teaches a method for state-less authentication, wherein Bisbee discloses IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires (see column 11, lines 1-7 'The Security Context and the symmetric session encryption key contained therein are then forwarded to the User and retained for the period for which the Security Context is valid.

In some instances, the Time-Offset and Expiration Time values may also be returned to the User, which allows the User to **renew** the Security Context prior to its **expiration** [i.e., IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires].', of Bisbee).

In addition, Bisbee further discloses a setting apparatus generating and transmitting common encryption keys to the process apparatuses to be used to encrypt and authenticate IP communications (see col. 10, line 66 to col. 11, line 4 'The Security Context Body is then encrypted using the Logon Component-specified symmetric or the generated private key [i.e., generating common encryption key] referenced by the respective Key Handle. The Security Context and the symmetric session encryption key [i.e., the common encryption key] contained therein are then forwarded to the User [i.e., transmitting the generated common encryption key, e.g. to the first and second IP process apparatuses] and retained for the period for which the Security Context is valid.', of Bisbee).

On the other hand, Park teaches a method for controlling an internet information security system in an IP packet level, wherein Park discloses the SPD (Security Processing Database) and SAD (Security Association Database) (see page 2, [0034] 'SPD' 'SAD', of Park)

iii. The ordinary skilled person would have been motivated to have applied the teaching of Sullenberger into the system of Arrow such that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit and dynamically establish an encrypted virtual private network, because Arrow teaches "VPN management station 160 controls VPN units 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100." (see column 6, lines 31-34, of Arrow, emphasis added). Sullenberger teaches "The invention relates more specifically to a method and apparatus for establishing a **dynamic** multipoint encrypted virtual private network (VPN)." (see column 1, lines 19-21, of Sullenberger, emphasis added). Therefore, Sullenberger's teaching could enhance Arrow's system.

The ordinary skilled person would have been motivated to have applied the teaching of Bisbee into the system of Arrow such that a VPN unit retransmitts a request to the VPN management unit before a term of validity for the SA expires, because Arrow teaches defining Security Associations (SA) for a VPN unit (see figure 13, 1310 'define VPN parameters', of Arrow). Therefore, Bisbee's teaching could increase the network security for Arrow's system, because Bisbee requires a VPN unit retransmitts a request to the VPN management unit before a term of validity for the SA expires.

The ordinary skilled person would have been motivated to have applied the teaching of Park into the system of Arrow to include a SPD and SAD, because Arrow teaches defining Security Associations (SA) for a VPN unit using database which includes information reflecting the structure of virtual private networks supported by the system and the configuration of the VPN units supported by the VPN management station (see column 13, lines 60-64, of Arrow). Therefore, Park's teaching could enhance Arrow's system by including SPD and SAD for defining Security Associations (SA).

Referring to claim 17:

Arrow, Sullenberger, Bisbee, and Park teach the claimed subject matter: an IPsec setting method (see claim 21 above). They further disclose the IPsec processing apparatus receiving a message from an IPsec setting apparatus, and transmits a request for communicating with another IPsec processing to the IPsec setting apparatus (see e.g. figure 8, 818 'create security context and provide to user', 820 'submit request for access and security context', of Bisbee).

Response to Arguments

5. Applicant's arguments, filed on July 28, 2011, have been fully considered, but they are not persuasive.

(a) Applicant argues:

"Neither Arrow nor Sullenberger disclose that the IPsec setting server generates and distributes the generated common secret key, and even if combined, do not disclose or suggest the feature of claim 1 of "said iPsec setting apparatus generates the common encryption key to be used in encryption and authentication of the IPsec communications between the first IPsec processing apparatus and the second IPsec processing apparatus and transmits the generated common encryption key to the IPsec processing apparatus." (see page 10, last paragraph).

Examiner maintains:

Arrow discloses "VPN management station [i.e., IP setting apparatus] 160 controls VPN units [i.e., IP process apparatuses] 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100.", "Configuration data includes information used to operate VPN unit 115, such as: an IP address of the unit, IP addresses of VPN endstations that will be transmitting data through the unit, the encryption algorithm [i.e., including the generated encryption key] to be used, the authentication algorithm to be used,", and "RSA module 722 supports management of encryption keys [i.e., included in the configuration data] and loading of configuration information into VPN unit 115 from VPN management station 160 (from FIG. 1)." (see col. 6, lines 31-34; col. 9, lines 35-40; and col. 11, lines 27-30, of Arrow). Therefore, Arrow discloses that the VPN management station (IP setting apparatus) generates and transmits encryption keys to the first and second VPN units (IP process apparatuses) to be used to encrypt and authenticate IP communications between the first and second VPN units (IP process apparatuses). However, Arrow does not explicitly disclose the common encryption key.

Sullenberger further discloses "establishing a shared secret [i.e., generating and transmitting the common encryption key] between the two endpoints" (see col. 2, lines 24-29, of Sullenberger), and "the encryption methodology is DES [i.e., DES (Data Encryption Standard) using the common encryption key]" (see col. 7, lines 44-47, of Sullenberger). Therefore, Sullenberger discloses generating and transmitting the

common encryption key. Therefore, Arrow, in combination with Sullenberger, disclose that the IP setting apparatus generates and transmits common encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses.

In addition, Bisbee further discloses "The Security Context Body is then encrypted using the Logon Component-specified symmetric or the generated private key [i.e., generating common encryption key] referenced by the respective Key Handle. The Security Context and the symmetric session encryption key [i.e., the common encryption key] contained therein are then forwarded to the User [i.e., transmitted the generated common encryption key, e.g. to the first and second IP process apparatuses] and retained for the period for which the Security Context is valid." (see col. 10, line 66 to col. 11, line 4 of Bisbee). Therefore, Arrow, in combination with Bisbee, also disclose that the IP setting apparatus generates and transmits common encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses.

Thus, the references disclose that the IP setting apparatus generates and transmits common encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses, such as claimed.

Conclusion

6. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached at 571-272-4006. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Joseph Pan/
Examiner, Art Unit 2492
September 12, 2011

/saleh najjar/

Supervisory Patent Examiner, Art Unit 2492